REMARKS:

Claims 105, 107, 109-115, 117, 118 127-156, 159, 162-166 and 168-185 were pending in the application. Claims 131, 132, 170, 173, 176, 179 have been canceled. Claims 105, 107, 115, 127, 128, 139-150, 152-156, 159, 163-166, 177, 178, 180-182 have been amended. Therefore, claims 105, 107, 109-115, 117, 118 127-130, 133-156, 159, 162-166, 168, 169, 171, 172, 174, 175, 177, 178, 180-185 are now pending in this application.

Support for the amendment to claims 105, 115, 127, 128, and 152 can be found throughout the specification, including but not limited to, page 10, line 21 through page 11, line 1. Support for the amendment to claim 107 can be found throughout the specification, including but not limited to, page 15, lines 21-23.

Examiner Interview

Applicant's undersigned representative conducted a telephone interview with the Examiner on October 13, 2009. Also participating in the call was Mr. Delos Larson. The undersigned presented arguments that the approach embodied by claim 105 differs from the signature-based approach of Chess and the event-based approach of Kouznetsov (that is, waiting for a program to take some action before classifying it). The substance of Applicant's arguments is reflected in the remarks below. While no agreement was reached, the Examiner indicated that an amendment similar to the amendment of claim 105 presented herein would likely overcome the current rejection.

Claim 105

The Examiner rejected independent claim 105 based on a proposed combination of Kouznetsov (U.S. Patent No. 6,973,577) and Chess (U.S. Patent No. 6,772,346). Applicant respectfully disagrees with these rejections, but has amended claim 105 to advance prosecution.

Claim 105 recites "selecting an active computer program," "executing each of a first and second plurality of detection routines," and "upon completing the executing of the first and second plurality of detection routines, using at least one of the first and second scores to categorize the code under investigation." As previously argued, this sequence of events is

neither taught or suggested by Kouznetsov, which can be considered to have an "event"-based approach to malicious code detection (i.e., Kouznetsov's analyzer 19 waits for system calls to be made by the code under investigation, and then intercepts/analyzes such calls).[1] In contrast, the method of claim 105 selects an active program, executes each of the recited first and second plurality of detections routines, and, upon completion, categorizes the code under investigation using results of the executed detection routines. Also as previously argued, Chess is not directed to analysis of an "active program" as in claim 105; rather, the reference is merely concerned with checking of a "file [that] arrives at a node." *See* Chess at 6:7-8. As such, the proposed combination of Kouznetsov and Chess is not believed to teach or suggest each and every feature of amended claim 105.

Furthermore, the Office Action could arguably be read to assert that the static analyzer 52 and dynamic analyzer 53 of Kouznetsov correspond to claim 105's "first plurality of detection routines" and "second plurality of detection routines," respectively. As explained in Applicant's Response to Office Action dated September 21, 2007, as well as the interview of October 13, 2009, Kouznetsov's analyzers 52 and 53 are both concerned only with what Kouznetsov calls "suspicious" events. *See* Kouznetsov 4:59-5:3. Accordingly, nothing in Kouznetsov can be said to correspond to "first plurality of detection routines" recited in claim 105, which are "executable to determine whether the selected code under investigation has characteristics and behaviors usually associated with a *valid* program.[2]

Chess is also cited by the Examiner. While Chess teaches checking a *file* (not an "active program") against known non-malicious and malicious files in steps 320 and 340, respectively, Chess at 6:8-21, this disclosure does not constitute "applying *each* of the first *plurality* of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results" and "applying *each* of the second *plurality* of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results" as in claim 105. Claim 105 refers to both a "first plurality of results [i.e., at least two results]" and

[1] Because Kouznetsov utilizes an event-based approach, there is no "selecting" of "an active program as code under investigation," followed by "applying" each of the first and second pluralities of detection routines to the code under investigation, as in claim 105.

[2] Applicant further submits that it is not clear whether programs under test in Kouznetsov (e.g., applications 33, 34 and 35) are "running on an operating system of the computer system," given that monitor/analyzer "functions as a

a "second plurality of results [i.e., at least two results]." Chess does not teach or suggest these features. Chess appears to have a single routine (exemplified by Fig. 3) that checks databases 210 and 220—Chess therefore cannot be said to have a first or second *plurality* of results as recited in claim 105. Chess certainly includes no teaching regarding "weighting" of the "first" and "second" pluralities of results as recited in claim 105.

Accordingly, Applicant submits that neither Kouznetsov nor Chess teaches the "first" or "second" plurality of detection routines of claim 105. Accordingly, even if there were motivation to combine these references in the manner suggested by the Examiner (which Applicant in no way concedes), the resultant combination would not include each and every limitation of claim 105. Accordingly, the proposed combination of Kouznetsov and Chess cannot be used to establish a *prima facie* case of obviousness with respect to claim 105. *See* MPEP § 2143.03. Further, Applicant respectfully submits that the Examiner has not adequately explained why one of ordinary skill in the art would be motivated to modify Kouznetsov in view of Chess, or what such a modification would look like.

For at least the reasons stated above, Applicant submits that claim 105 is patentably distinct over the cited references. Claim 105's dependent claims are patentably distinct over the cited references at least by virtue of their dependency on claim 105. Independent claims 115, 127, 128, 152, and 159 are believed to be patentably distinct (along with their respective dependent claims) for at least reasons similar to those provided above in support of claim 105.

Claim 107

As also argued in the interview, Applicant submits that the Kouznetsov-Chess combination does not teach or suggest the features of amended claim 107, in which "said method is performed repeatedly until a plurality of active programs on the computer system have been categorized with respect to their likelihood of compromising the security of the computer system." In contrast, Kouznetsov describes an approach in which the static and dynamic analyzers wait until an "occurrence[] of a monitored event[]" happens. *See Kouznetsov* at col. 4,

---

logical 'shim' interposed between the operating system 32 and each of the applications 33, 34, and 35." Kouznetsov at 4:15-25.

line 17. For at least this reason, Applicant submits that claim 107 is further patentably distinct over the cited references.

Claim 136

The Office Action does not appear to address the precise language of this claim, which recites "wherein the determination is made based on the first score exceeding a valid code threshold value, regardless of the second score." For at least this reason, Applicant submits that claim 136 is further patentably distinct over the cited references, along with claims 143, 148, 155, 164.

Claim 168

The Office Action addresses this claim at page 12, but merely cites to two columns of text in Kouznetsov. Applicant submits that the Office Action does not specifically explain how this portion of Kouznetsov's disclosure teaches or suggests the limitations of claim 168. For at least this further reason, Applicant submits that claim 168 is further patentably distinct over the cited references, along with claims 171, 174, 177, 180, and 183.

Claim 169

The Office Action addresses this claim at page 12, but merely cites to two columns of text in Kouznetsov. Applicant submits that while Kouznetsov teaches receiving information via a system call, the "static analyzer" and "dynamic analyzer" of Kouznetsov, alleged by the Examiner to be the first and second pluralities of detection routines, do not themselves "obtain[] information about the code under investigation by accessing the operating system of the computer system via an API of the operating system." For at least this further reason, Applicant submits that claim 169 is further patentably distinct over the cited references, along with claims 172, 175, 178, 181, and 184.

Applicant therefore respectfully requests removal of the § 103 rejections.

CONCLUSION:

Applicants submit the application is in condition for allowance, and an early notice to that effect is requested.

If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above-referenced application from becoming abandoned, Applicant hereby petitions for such extension.

The Commissioner is authorized to charge any fees that may be required, or credit any overpayment, to Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C. Deposit Account No. 501505/6002-00602/DMM.

Respectfully submitted,

Date: October 16, 2009

By: /Dean M. Munyon/
Dean M. Munyon
Reg. No. 42,914

Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P. O. Box 398
Austin, Texas 78767
(512) 853-8847